Longhorn Client Security

Paul J. Leach
Windows Security Architect
Microsoft Corporation

Microsoft

Agenda

- Longhorn Security

Agenda

- Longhorn Security
  - Customer feedback
  - Security pillars
    - Engineering Excellence
    - Isolation & Resiliency
    - Security Management
    - Authentication, Authorization, and Audit
- Summary

Responding to Customer Feedback

Feedback and Trends

- Constant threat of hackers, viruses and malware
- Patching takes too much time and resources
- High cost of lost productivity and downtime
- Need responsive and powerful operating system for critical tasks

Responding to Customer Feedback

Feedback and Trends

- Constant threat of hackers, viruses and malware
- Patching takes too much time and resources
- High cost of lost productivity and downtime
- Need responsive and powerful operating system for critical tasks

Protecting Against and Responding to Security Threats

Security vulnerabilities have increased desktop TCO on the order of $200 per user per year, or about 4% for unmanaged PCs (Source: Gartner)

Longhorn Goal

The secure and reliable foundation you can count on to keep your PCs running, data protected and users productive

Longhorn Security Pillars

Engineering excellence	Advanced security practices, internal tools, and guidance as part of core Windows development
Isolation & Resiliency	A platform that is resilient in the presence of security threats and reduces the risk of business interruption
Security Management	Scalable, centralized security monitoring of desktops in the enterprise
Authentication, Authorization, and Audit	Enable seamless protection of information and resources through validated access by authorized users and applications

Engineering Excellence

- Improved development process, following Security Development Lifecycle
  - Threat modeling for known and projected threats
  - Internal security team reviews built into schedule
  - More penetration testing
  - Prefix/Prefast to scan code for vulnerabilities, before it's ever checked in to the build
    - SAL annotations for cross-procedural analysis
  - Training and guidance for development team on writing secure code
  - Code coverage requirements
  - Banned APIs

Isolation & Resiliency

- System starts and runs in a known good state
  - Secure Startup protects offline attacks on boot loader
  - Full Volume Encryption to protects entire disk including sensitive registry and OS files when OS is offline
  - Code integrity protects OS when it's running
    - All Windows system code is signed
    - Loader checks integrity of each file on load
- Limited User Accounts "just work"
  - Legacy applications run under lower privileges without reconfiguration with file/registry virtualization
  - Interfaces and UI for reduced-privilege execution

Enhanced Security Services through Hardware

Secure Startup addresses the lost or stolen laptop scenarios with TPM-rooted integrity and encryption.

- Provides the foundation for security by ensuring that your PC starts in a good known state.
- Ensures that core OS files were not tampered with during an offline attack.
- Protects encrypted files from software based attacks.

Hardware Requirements

Hardware Requirements

- Trusted Platform Module (TPM) v 1.2
  - Provides platform integrity measurement and reporting
  - Requires chipset support for secure TPM interface

Hardware Requirements

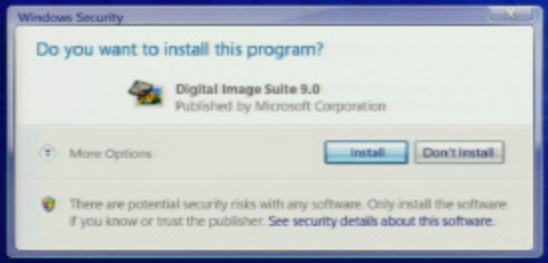
- Trusted Platform Module (TPM) v 1.2
  - Provides platform integrity measurement and reporting
  - Requires chipset support for secure TPM interface
- BIOS/Extensible Firmware Interface – Trusted Computing Group (TCG) compliant
  - Establishes chain of trust for pre-OS boot
  - Must support TCG specified Static Root Trust Measurement (SRTM)
    - See www.trustedcomputinggroup.org

Limited User Accounts

- Improves overall security and manageability by limiting need for, and usage of, administrative privilege
- All users normally operate without admin privileges, even if they have an admin-enabled account
- UX for allowing admin to run an application within a limited user's session
- File/registry virtualization allows legacy applications to run without admin privileges

Limited User Software Install

Limited User Software Install

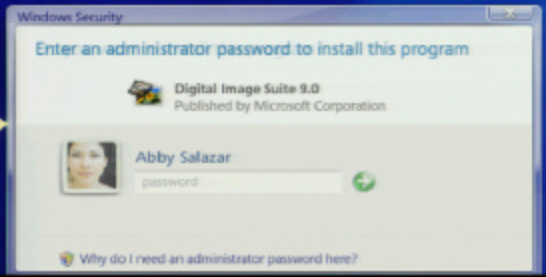


Limited User starts new program installation

Limited User Software Install

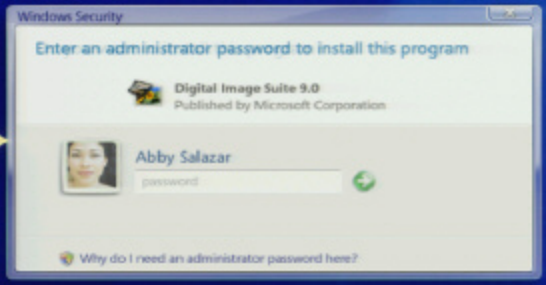
Limited User Software Install

User is prompted for credentials with permission to install

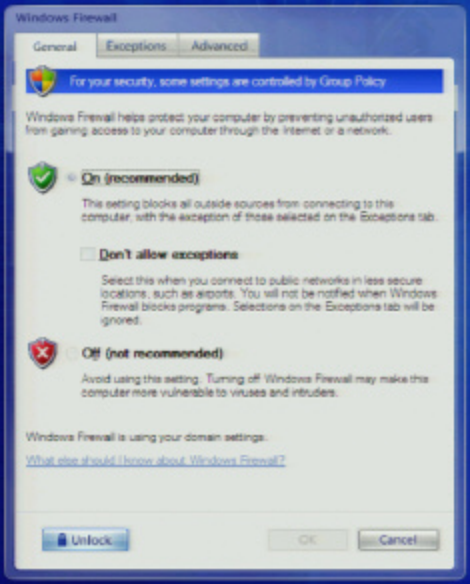


Limited User Software Install

User is prompted for credentials with permission to install

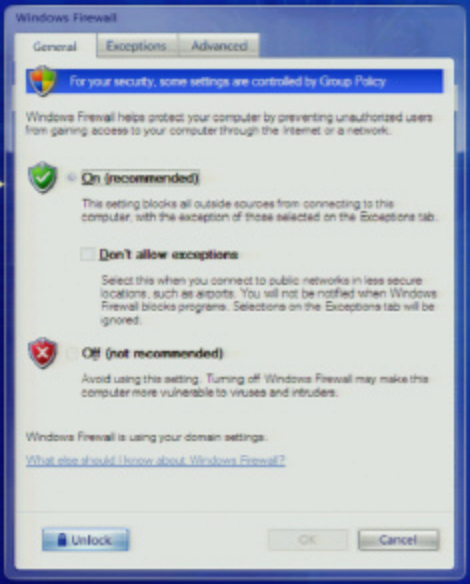


Security Experience – Limited User

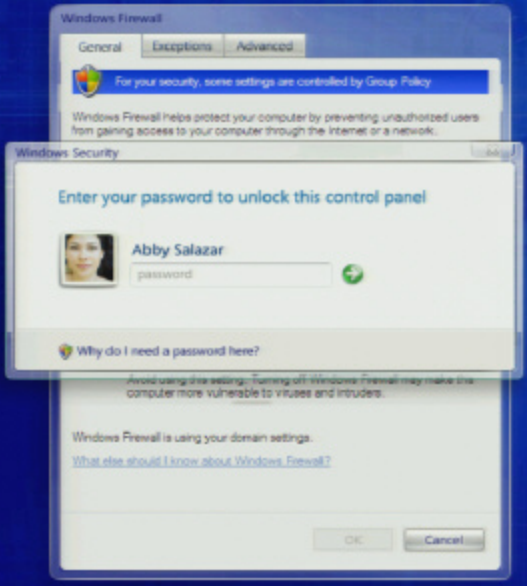


Security Experience - Limited User

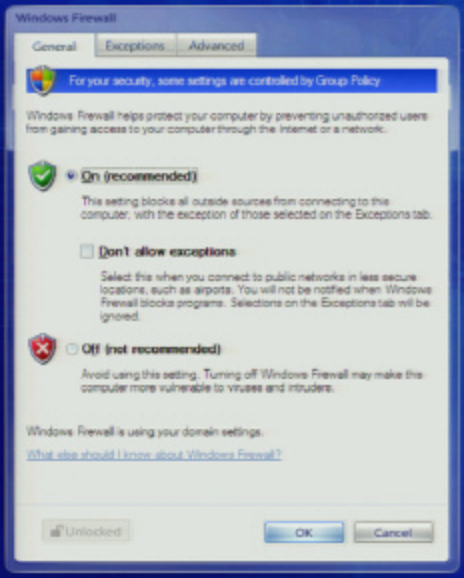
Firewall settings are locked down (grayed out)



Security Experience – Limited User



Security Experience – Limited User



Security Experience – Limited User

Settings are now available to be changed

Isolation & Resiliency (Continued)

- Trustworthy Browsing
  - Browser lockdown and privacy controls
- Additional resiliency against malware attacks
  - Hardening of Windows services, using a allow-list of allowed actions and enforcing those actions
  - Spyware detection and cleaning

IE7 Security Enhancements

- IE vulnerabilities are distributed between vulnerable core code paths like file download and script engine hosting, vulnerable extensibility like ActiveX and more general security bugs like buffer overruns.
- XP SP2 addressed the most dangerous abuses of script engine hosting with LMZL and some file download scenarios but did not address all vulnerability classes.
- IE7 security mitigations target all known remaining threats such as ActiveX repurposing, URL Parsing, XDomain, Drag/Drop and Buffer Overruns.
- IE7 will also have more have visible protections like an improved SSL UX with Anti-phishing notifications and tools to clear browsing history.

IE7: Security & Privacy

Confidence in secure browsing

Reduce impact of malware

- Runs with limited permissions, reduces attack surface
- Simplified architecture to defend against exploits
- "Reset to factory settings" option

Safely add new browser functionality

Full control over extensibility

- Prompt user first time any extension is run
- Safe mode allows IE to run without extensions
- Automatically disable unreliable add-ons
- Monitor add-on speed, option to disable slow ones

Personal information stays private

Protection of personal data

- Highlight secure sites, warn if personal data in the clear
- Notification when a site exhibits suspicious behavior
- Warn when browsing to known spoofing sites
- "No tracks" browsing, one-click cleanup of cache

Anti-Spyware

- Protection from malicious and suspicious software
- Discovers suspicious or bad software via signatures
- Cleans up malware messes in systems
- Commitment to detect & clean spyware in Longhorn.

Security Management

- Network access protection for health check of machines, both LAN and VPN
  - Dependent upon Longhorn server
- Reboots for patches reduced up to 70%
  - Hotpatching
  - Restart manager
- Client-based security scanning agent
  - Consistent report of security configuration and patch status
  - Utilizes WUS agent for patch status
- Control over installation of USB Flash Drives

Security Management

- Network access protection for health check of machines, both LAN and VPN
  - Dependent upon Longhorn server
- Reboots for patches reduced up to 70%
  - Hotpatching
  - Restart manager
- Client-based security scanning agent
  - Consistent report of security configuration and patch status
  - Utilizes WUS agent for patch status
- Control over installation of USB Flash Drives

Anti-Spyware

- Protection from malicious and suspicious software
- Discovers suspicious or bad software via signatures
- Cleans up malware messes in systems
- Commitment to detect & clean spyware in Longhorn.

Security Management

- Network access protection for health check of machines, both LAN and VPN
  - Dependent upon Longhorn server
- Reboots for patches reduced up to 70%
  - Hotpatching
  - Restart manager
- Client-based security scanning agent
  - Consistent report of security configuration and patch status
  - Utilizes WUS agent for patch status
- Control over installation of USB Flash Drives

Security Management (Continued)

- Integrated IPSEC/Firewall management
  - Simplified interface for network security management
- "Parental Controls" (actual name TBD) – applies in some corporate scenarios
  - Content filtering, restrict contacts for Email and IM, time restrictions, logging and reporting

Authentication, Authorization, and Audit

- Authentication
  - Enhanced smartcard support
    - EFS and RMS keys on smartcards
    - Deployment and user self-service tools
  - Winlogon rearchitecture
    - Allows additional authentication methods such as biometrics using Credential Providers instead of GINA replacement
    - Unified user experience for all credential entry
  - Crypto Next Generation
    - Improved cryptographic infrastructure allows easy integration of new algorithms and key management services to meet national requirements and evolving threats
  - PKI
    - Improved enrollment tools, key archival support, and key/certificate roaming
    - Peer trust for certificates
  - Castle
    - Replication of accounts and authentication data for small groups of machines

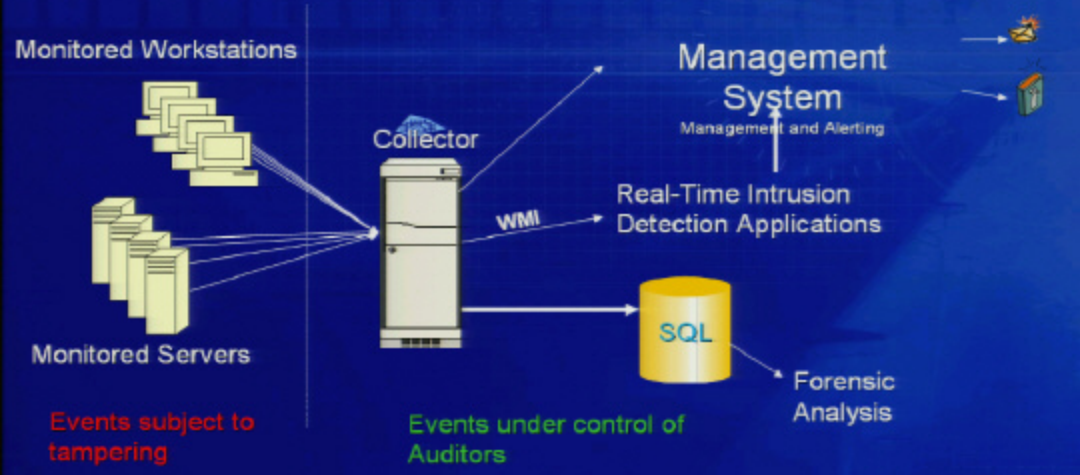
Authentication, Authorization, and Audit (Continued)

- Authorization
  - Authorization Manager (server dependent)
    - Improved support for application RBAC needs
    - Enhanced control over role definitions and role assignments
  - Web Services (Indigo/XSI)
    - Support for message authentication and confidentiality using Passwords, Kerberos, X.509, and SAML
    - Flexible trust, claims filtering, and authorization policies
- Audit
  - Finer-grained audit policy control using subcategory filters
  - Easier to interpret log entries using new event schema
  - MACS client to move security events off of local machine

Audit: MACS

- **Microsoft Audit Collection Service (MACS)**
  - Auditor-Administrator role separation
  - Distributed application to protect audits every step of the way from the security log to the database
  - Real-time and forensic analysis across multiple machines
  - Lightweight agent suitable to be run on workstations

Audit: MACS


Monitored Workstations
Collector
Management System
Management and Alerting
WMI
Real-Time Intrusion Detection Applications
SQL
Forensic Analysis
Monitored Servers
Events subject to tampering
Events under control of Auditors

Summary

- Windows Longhorn will introduce important new security advances
  - Providing greater protection of personal and corporate data from harm caused by hackers and malicious software
  - Protecting your privacy
  - Helps you easily secure your computers and your network, at home, at work, while traveling
- Combination of new software and hardware establishes a higher level of security

Microsoft®

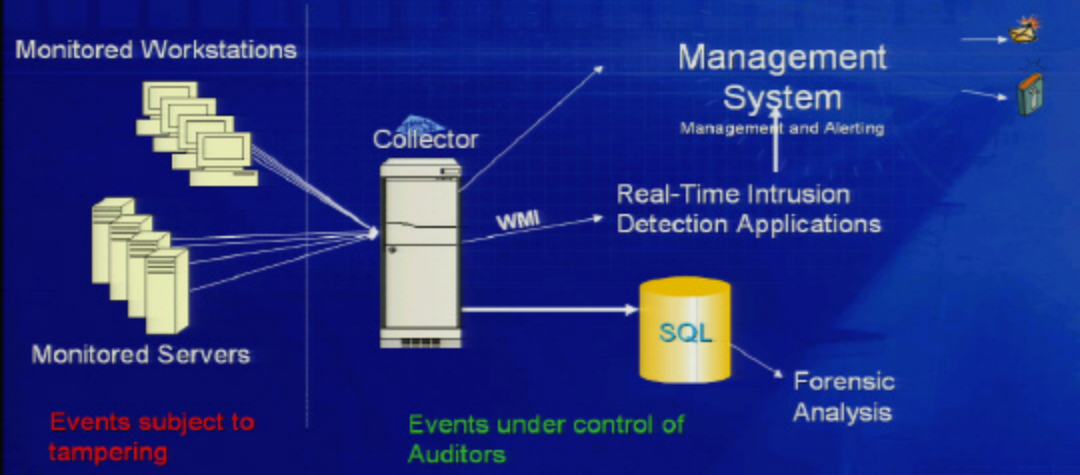
Your potential. Our passion.™

Microsoft

Summary

- Windows Longhorn will introduce important new security advances
  - Providing greater protection of personal and corporate data from harm caused by hackers and malicious software
  - Protecting your privacy
  - Helps you easily secure your computers and your network, at home, at work, while traveling
- Combination of new software and hardware establishes a higher level of security

Audit: MACS


Monitored Workstations
Monitored Servers
Collector
WMI
Management System
Management and Alerting
Real-Time Intrusion Detection Applications
SQL
Forensic Analysis
Events subject to tampering
Events under control of Auditors

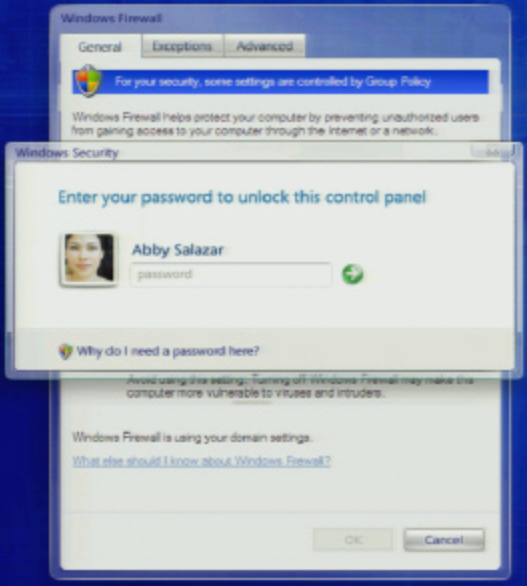
Authentication, Authorization, and Audit (Continued)

- Authorization
  - Authorization Manager (server dependent)
    - Improved support for application RBAC needs
    - Enhanced control over role definitions and role assignments
  - Web Services (Indigo/XSI)
    - Support for message authentication and confidentiality using Passwords, Kerberos, X.509, and SAML
    - Flexible trust, claims filtering, and authorization policies
- Audit
  - Finer-grained audit policy control using subcategory filters
  - Easier to interpret log entries using new event schema
  - MACS client to move security events off of local machine

Security Management (Continued)

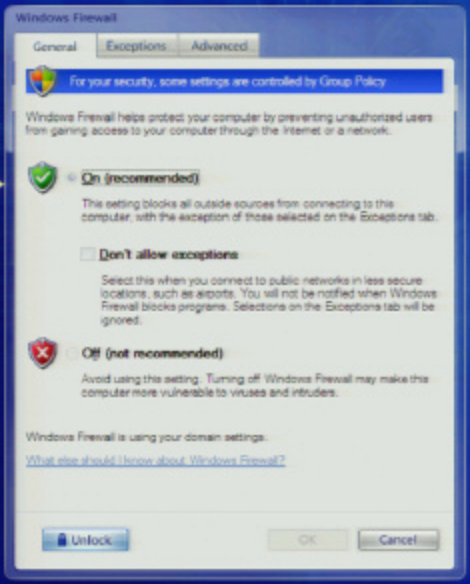
- Netw rated IPSEC/Firewall management mach
  - Dep plified interface for network security nagement
- Rebo ntal Controls" (actual name TBD) –
  - Hot es in some corporate scenarios
  - Res
- Client tent filtering, restrict contacts for Email and time restrictions, logging and reporting
  - Cor pat
  - Util
- Contr

Security Experience – Limited User



Security Experience - Limited User

Firewall settings are locked down (grayed out)



Responding to Customer Feedback

Feedback and Trends

- Constant threat of hackers, viruses and malware
- Patching takes too much time and resources
- High cost of lost productivity and downtime
- Need responsive and powerful operating system for critical tasks

Protecting Against and Responding to Security Threats

Security vulnerabilities have increased desktop TCO on the order of $200 per user per year, or about 4% for unmanaged PCs (Source: Gartner)

Longhorn Goal

The secure and reliable foundation you can count on to keep your PCs running, data protected and users productive